Fig.1.

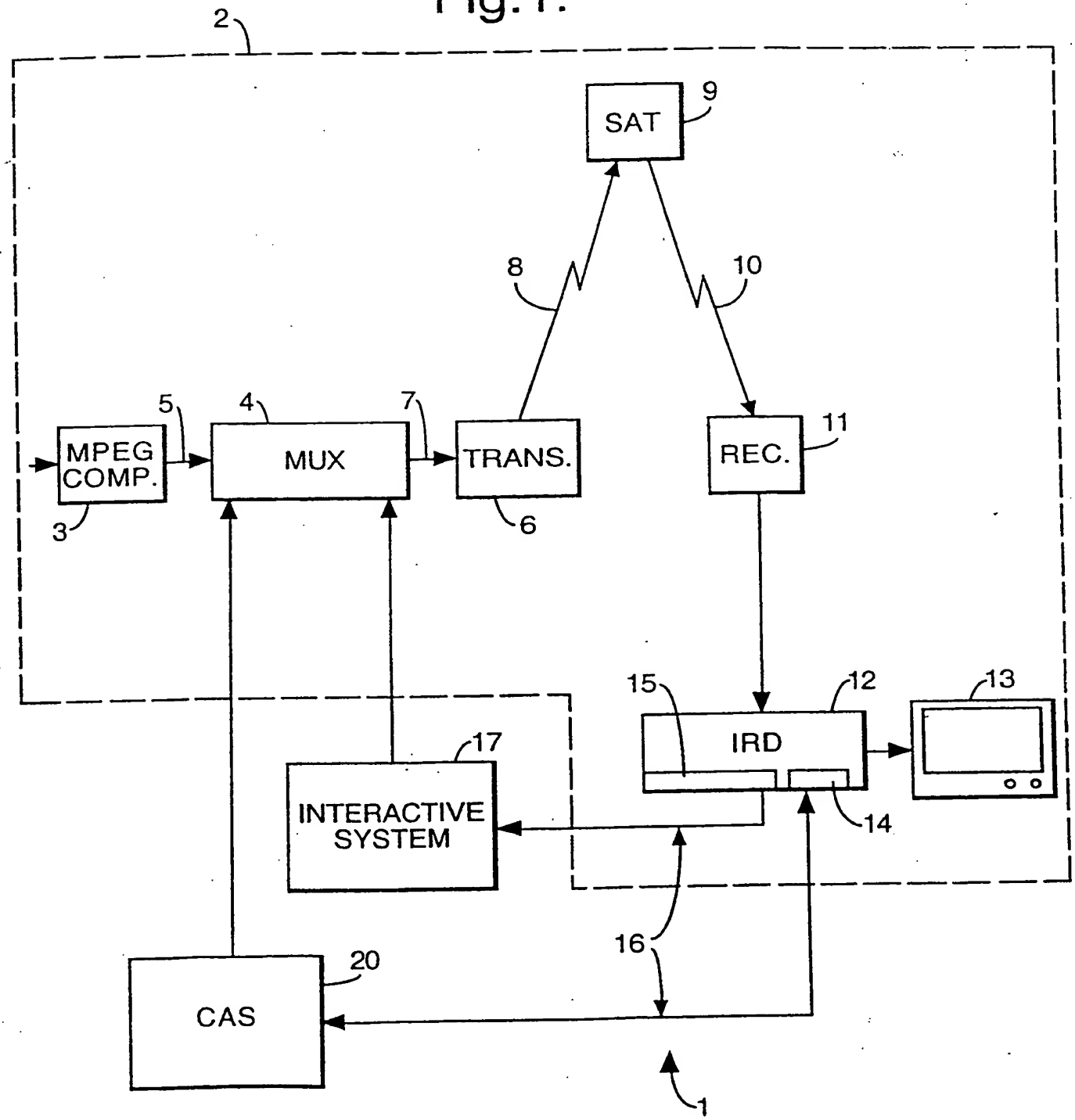

2
SAT
9
8
10
MPEG COMP.
5
3
MUX
4
7
TRANS.
6
REC.
11
15
IRD
12
13
14
INTERACTIVE SYSTEM
17
16
CAS
20
1

Fig.2.

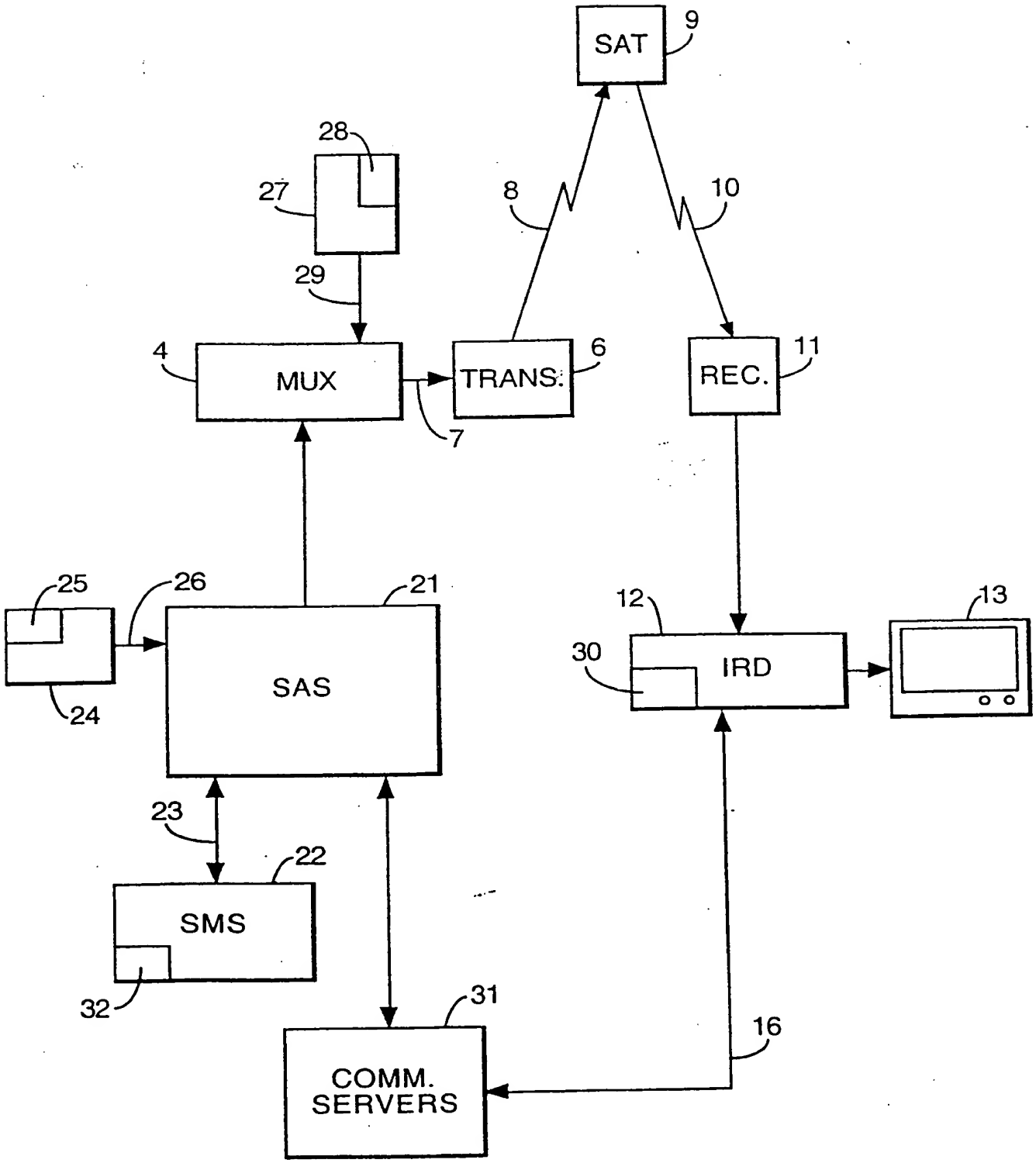
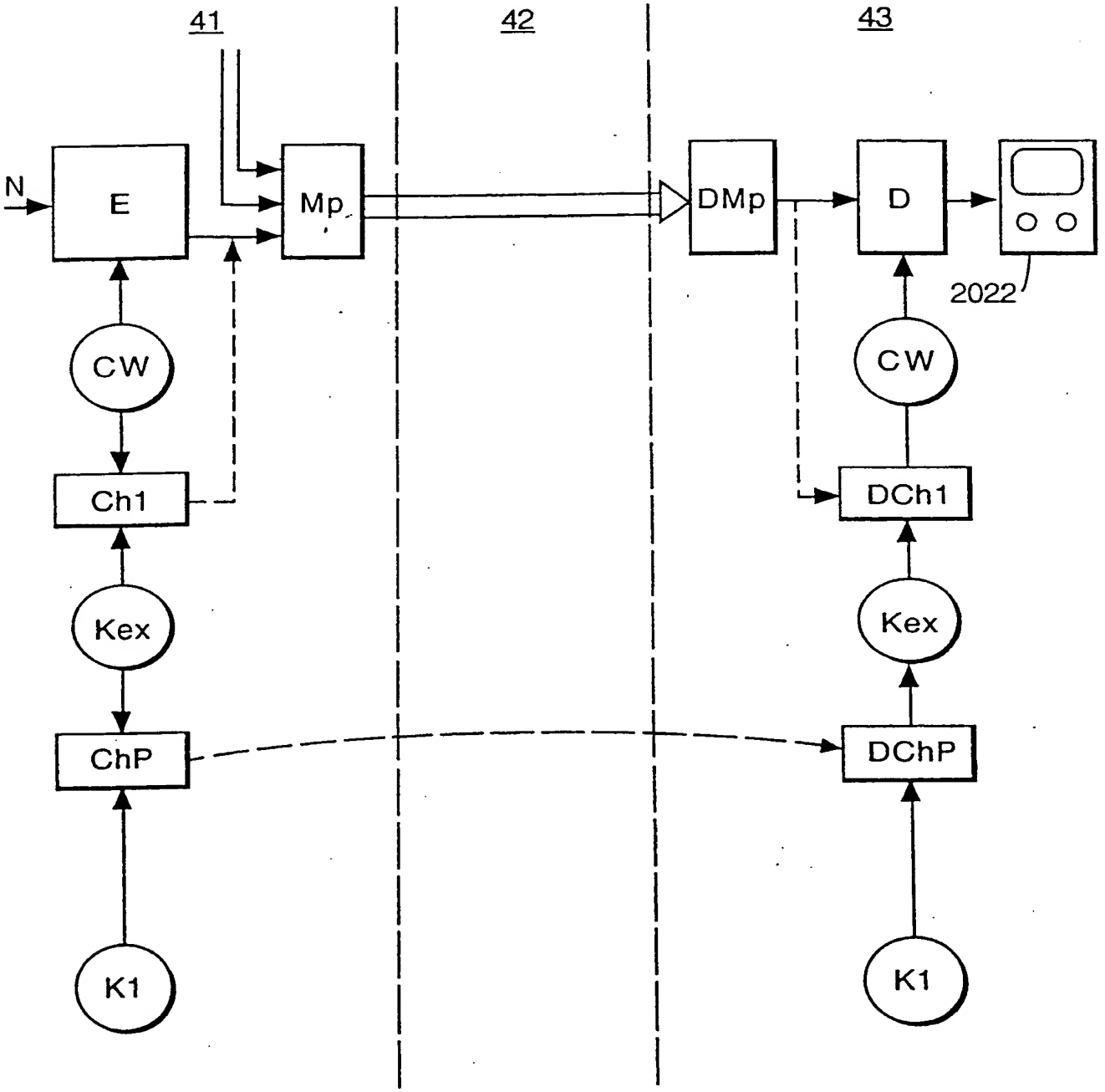
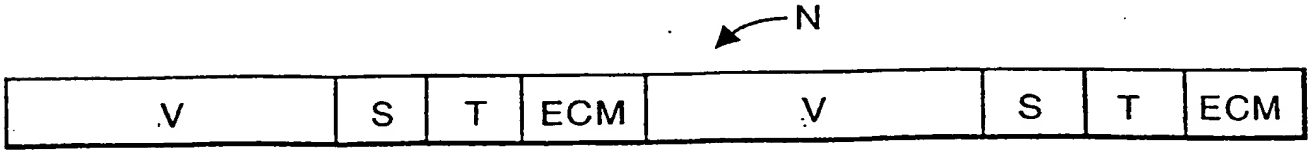

SAT
9
28
27
8
10
29
4
MUX
TRANS.
6
REC.
11
7
25
26
21
12
13
30
IRD
SAS
24
23
22
SMS
32
31
16
COMM.
SERVERS

Fig.3.


41
42
43
N
E
Mp
DMp
D
2022
CW
Ch1
Kex
ChP
K1
CW
DCh1
Kex
DChP
K1


N
V
S
T
ECM
V
S
T
ECM

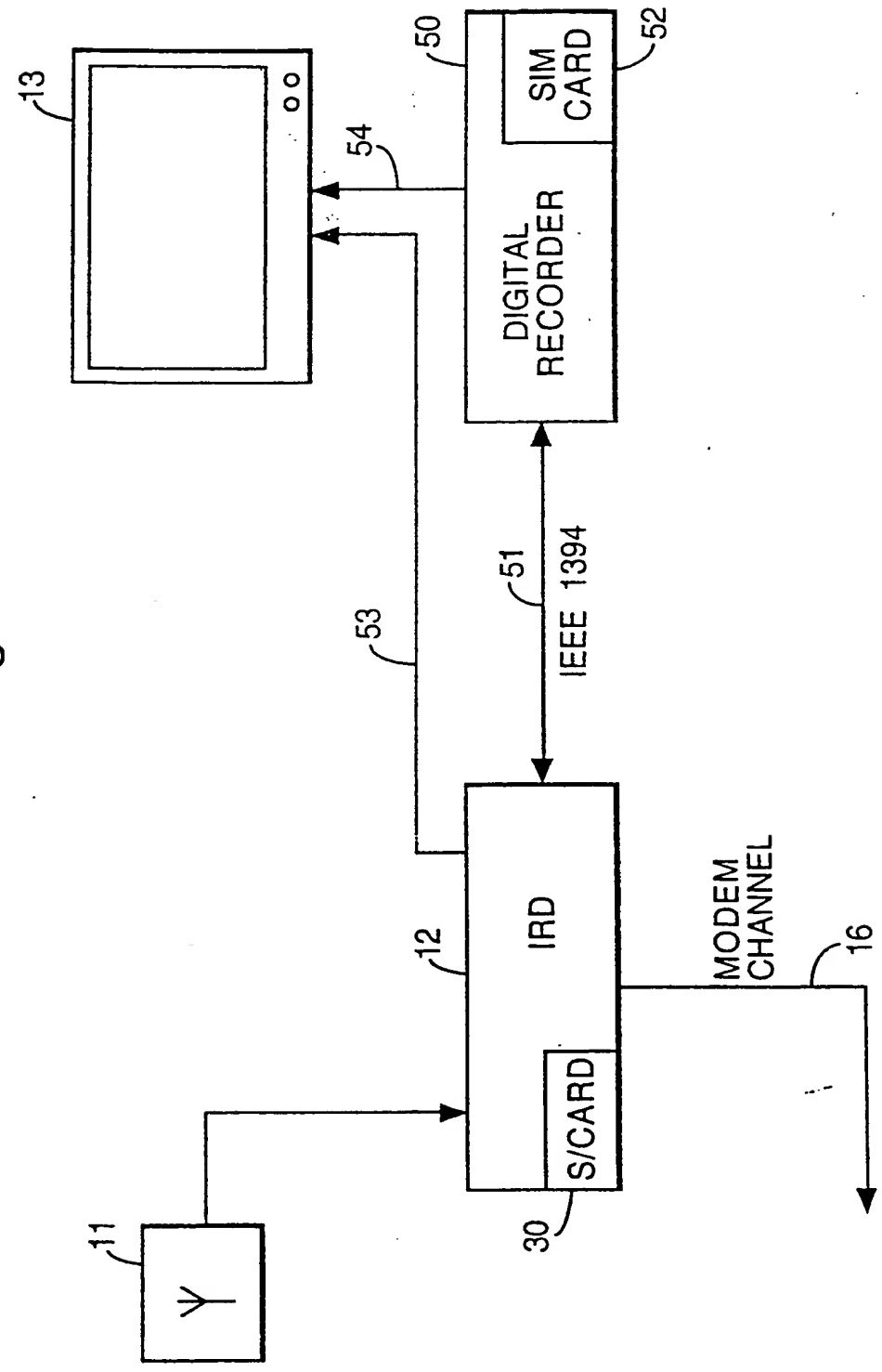

13
50
SIM CARD
52
54
DIGITAL RECORDER
51
IEEE 1394
53
12
IRD
MODEM CHANNEL
16
S/CARD
30
11

Fig.4.

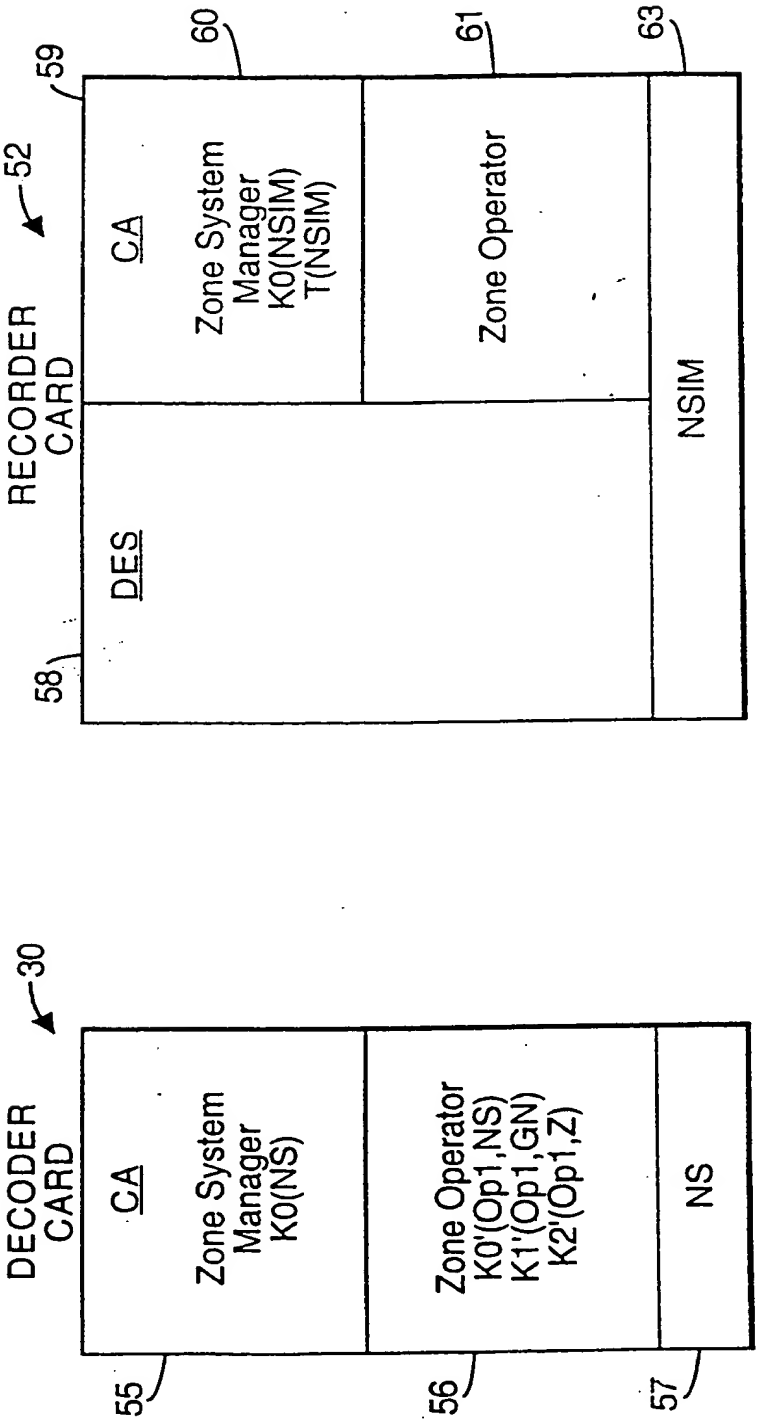

RECORDER CARD
52
59
60
61
63
CA
Zone System Manager K0(NSIM) T(NSIM)
Zone Operator
NSIM
DES
58
DECODER CARD
30
CA
Zone System Manager K0(NS)
Zone Operator K0'(Op1,NS) K1'(Op1,GN) K2'(Op1,Z)
NS
55
56
57

Fig.5.

Fig.6.

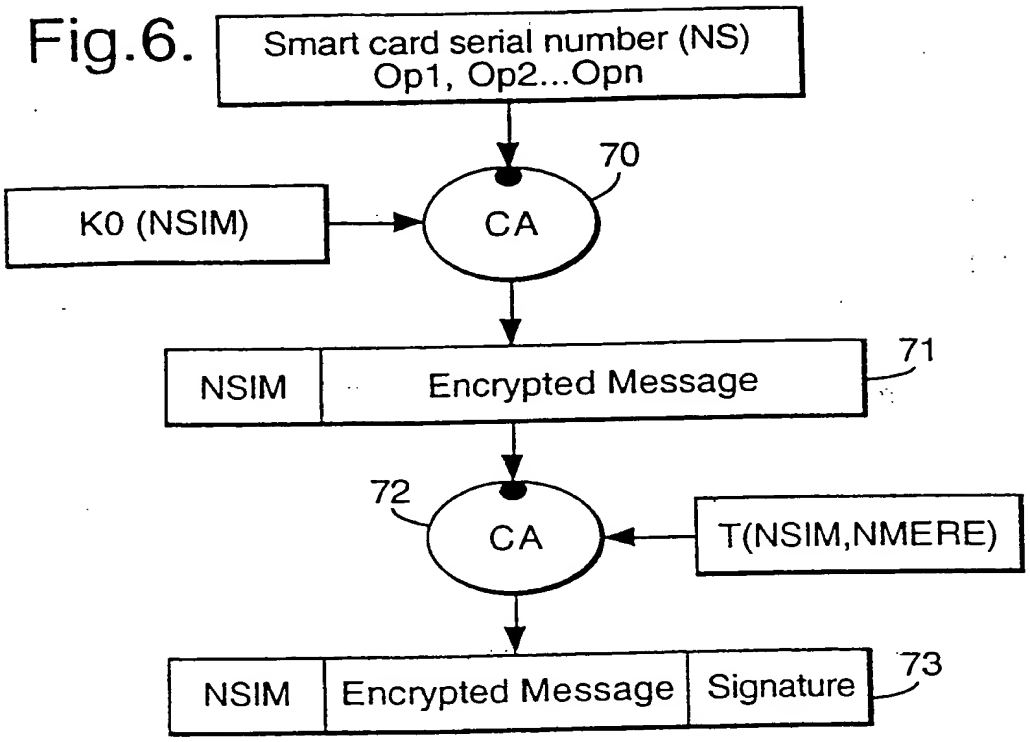

Smart card serial number (NS)
Op1, Op2...Opn
70
K0 (NSIM)
CA
NSIM
Encrypted Message
71
72
CA
T(NSIM,NMERE)
NSIM
Encrypted Message
Signature
73

Fig.7.

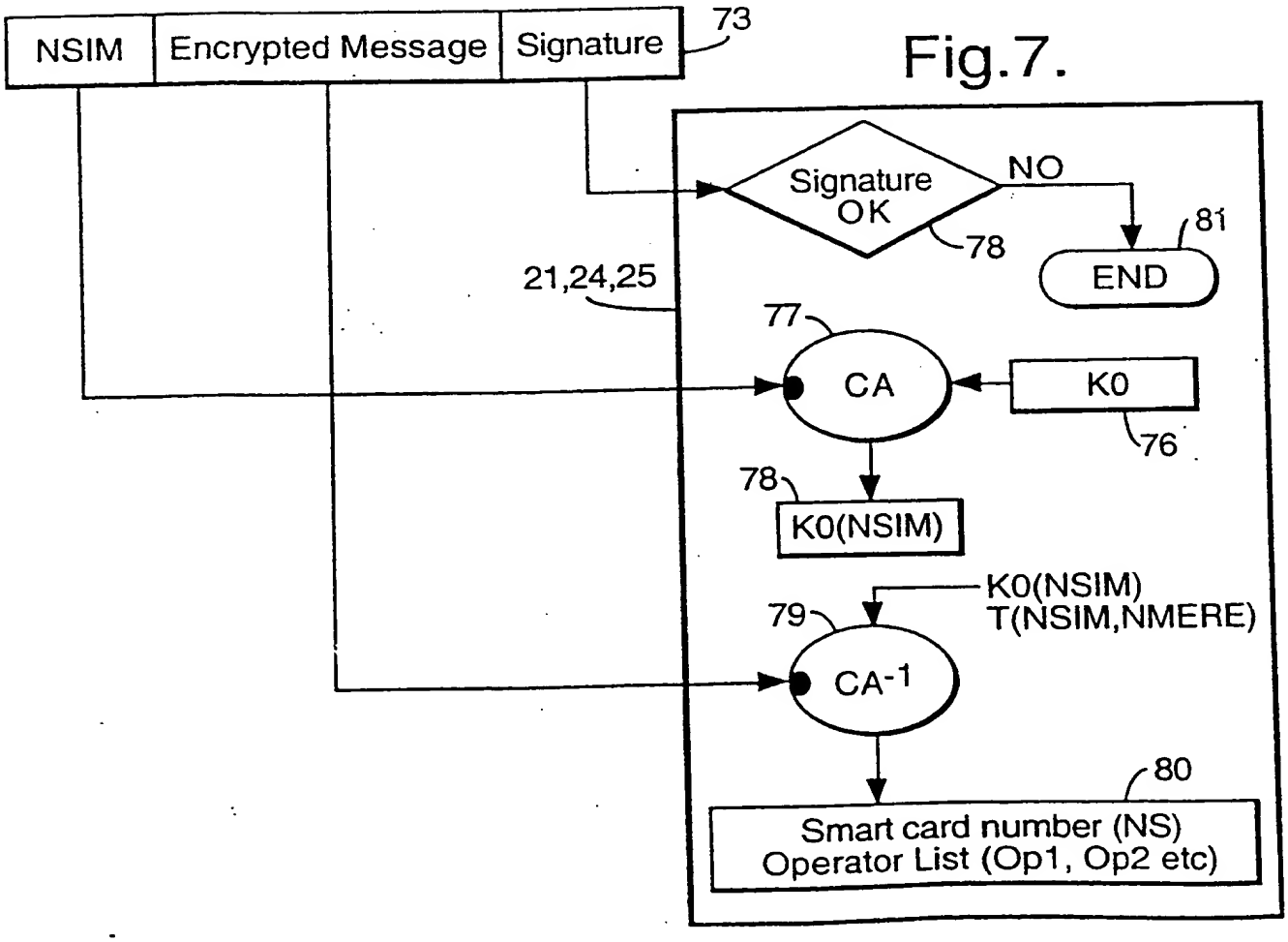

NSIM
Encrypted Message
Signature
73
Signature OK
NO
78
81
END
21,24,25
77
CA
K0
76
78
K0(NSIM)
K0(NSIM)
T(NSIM,NMERE)
79
CA-1
80
Smart card number (NS)
Operator List (Op1, Op2 etc)

Fig.8.

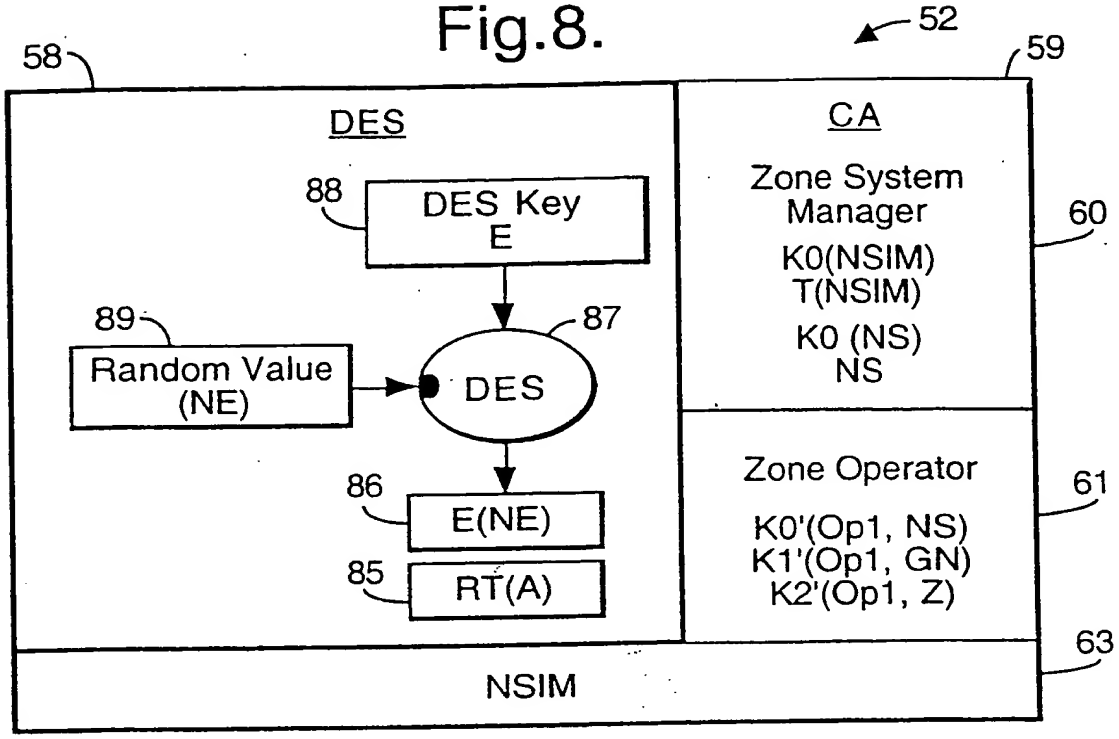

52
58
59
DES
CA
88
DES Key E
Zone System Manager
K0(NSIM)
T(NSIM)
K0 (NS)
NS
60
89
87
Random Value (NE)
DES
86
E(NE)
85
RT(A)
Zone Operator
K0'(Op1, NS)
K1'(Op1, GN)
K2'(Op1, Z)
61
63
NSIM

Fig.11.

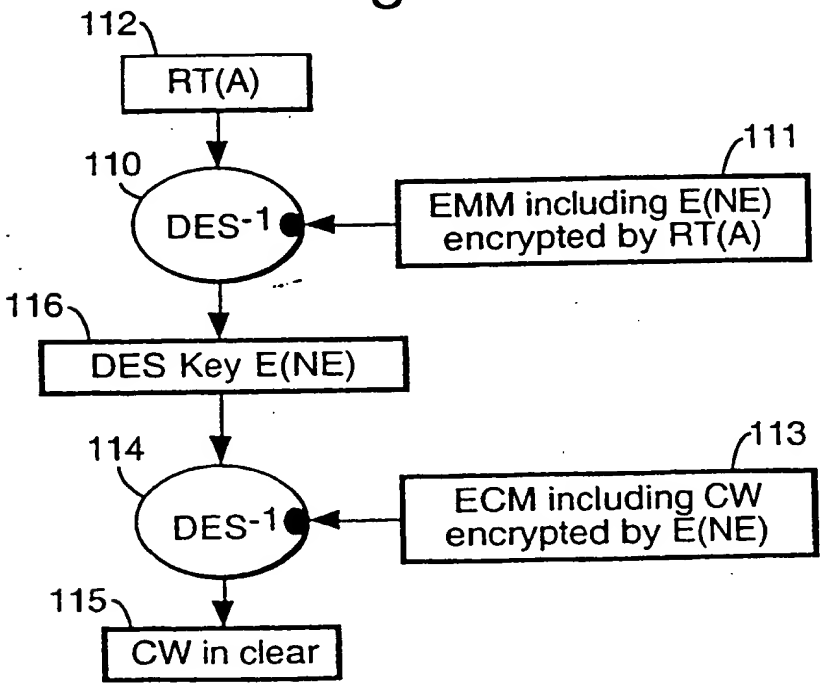

112
RT(A)
110
DES-1
111
EMM including E(NE) encrypted by RT(A)
116
DES Key E(NE)
114
DES-1
113
ECM including CW encrypted by E(NE)
115
CW in clear

Fig.9.

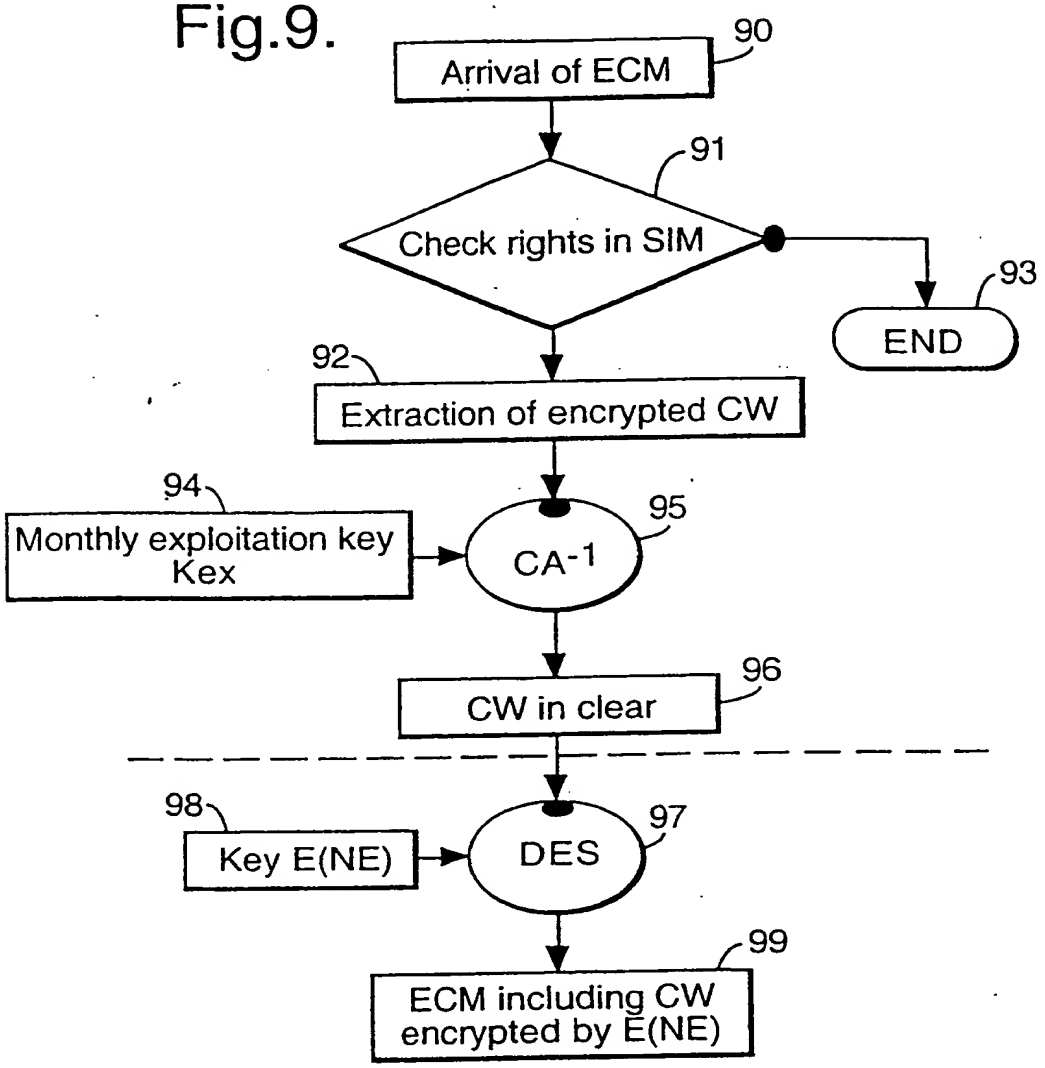

Arrival of ECM
90
Check rights in SIM
91
END
93
Extraction of encrypted CW
92
Monthly exploitation key Kex
94
CA-1
95
CW in clear
96
Key E(NE)
98
DES
97
ECM including CW encrypted by E(NE)
99

Fig.10.

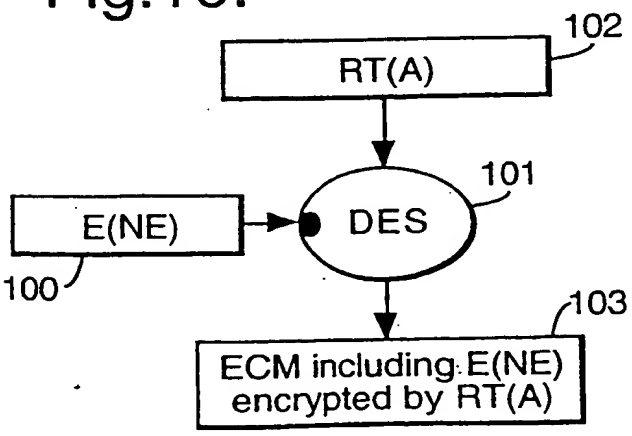
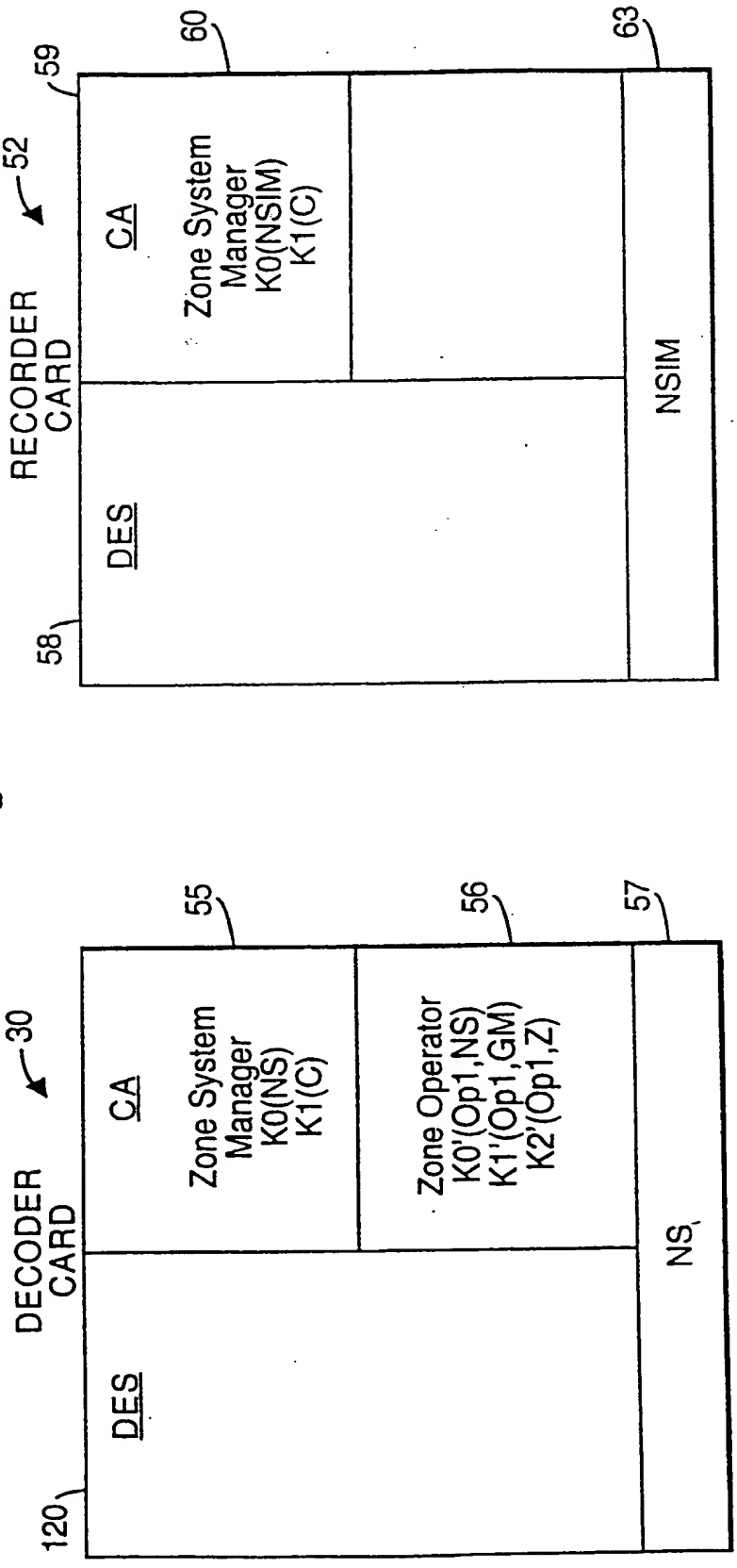

RT(A)
102
E(NE)
100
DES
101
ECM including E(NE) encrypted by RT(A)
103

Fig.12.


RECORDER CARD
52
59
60
63
CA
Zone System Manager K0(NSIM) K1(C)
DES
58
NSIM
DECODER CARD
30
55
56
57
CA
Zone System Manager K0(NS) K1(C)
Zone Operator K0'(Op1,NS) K1'(Op1,GM) K2'(Op1,Z)
DES
120
NS

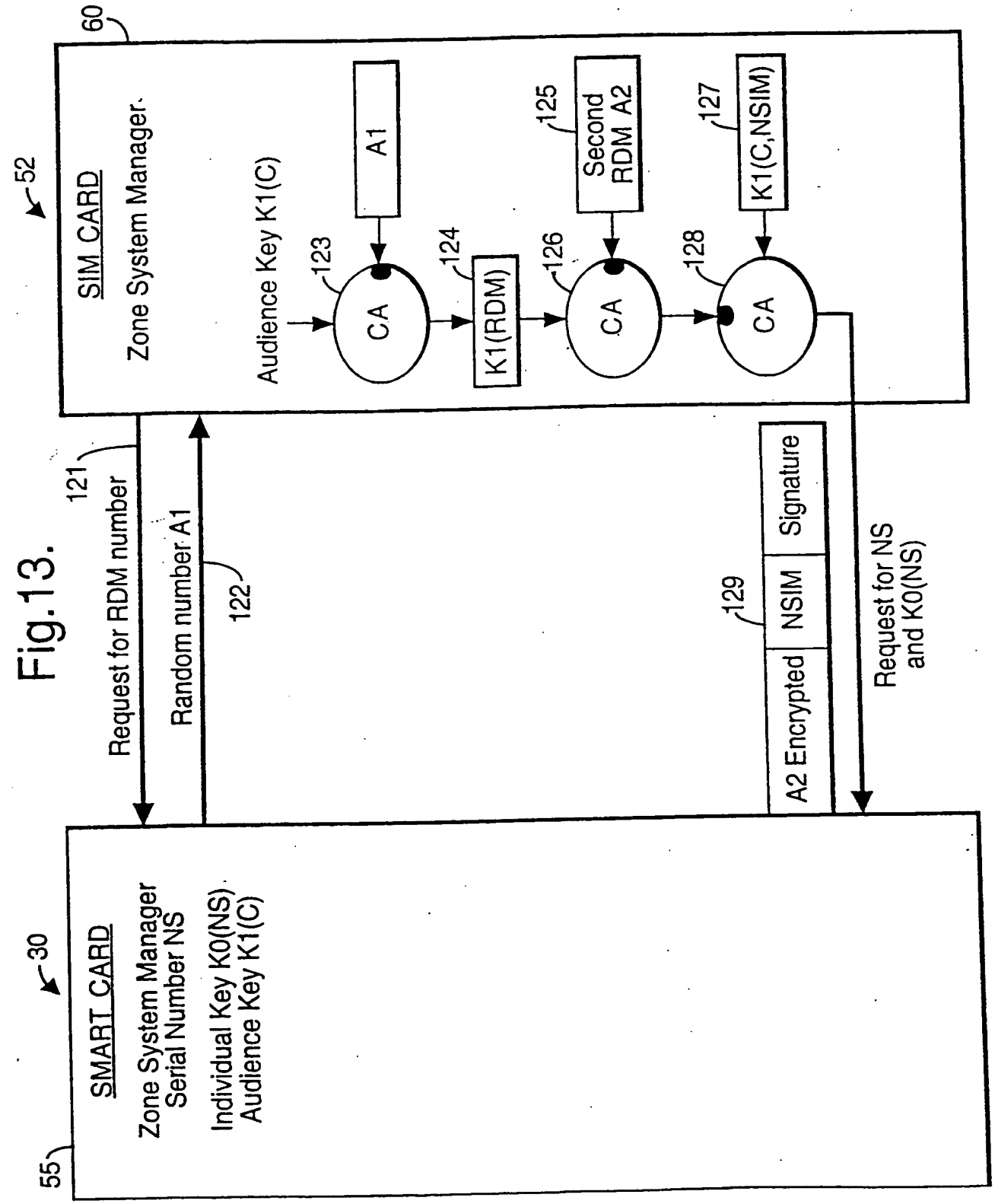

60
52
SIM CARD
Zone System Manager
Audience Key K1(C)
A1
123
CA
124
K1(RDM)
125
Second RDM A2
126
CA
127
K1(C,NSIM)
128
CA
121
Request for RDM number
Random number A1
122
129
A2 Encrypted
NSIM
Signature
Request for NS and K0(NS)
30
SMART CARD
Zone System Manager Serial Number NS
Individual Key K0(NS) Audience Key K1(C)
55

Fig.13.

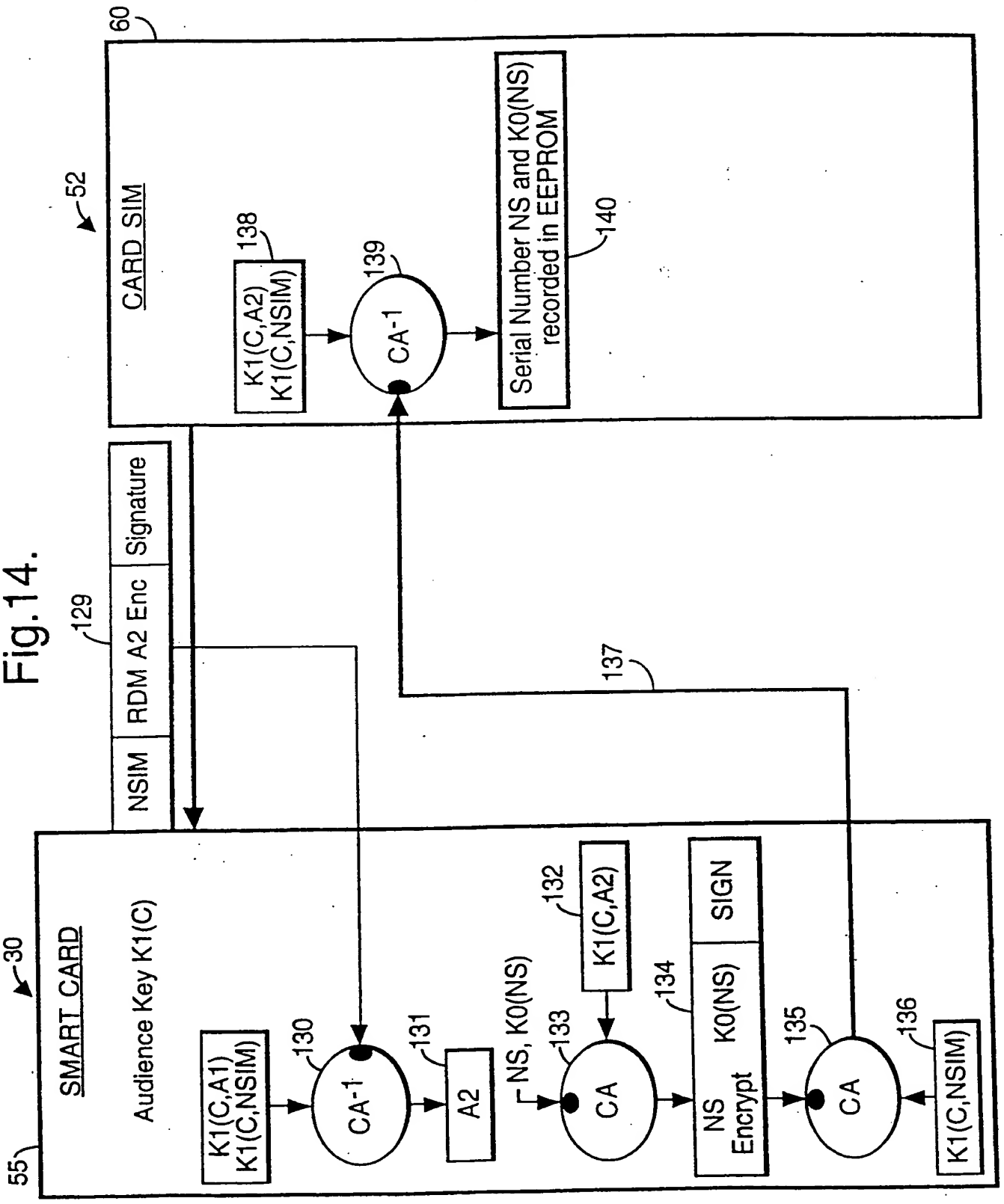

60
52
CARD SIM
K1(C,A2)
K1(C,NSIM)
138
139
CA-1
Serial Number NS and K0(NS)
recorded in EEPROM
140
129
NSIM
RDM A2 Enc
Signature
137
30
SMART CARD
Audience Key K1(C)
K1(C,A1)
K1(C,NSIM)
130
CA-1
131
A2
NS, K0(NS)
132
K1(C,A2)
133
CA
134
NS
Encrypt
K0(NS)
SIGN
135
CA
136
K1(C,NSIM)
55

Fig.14.

Fig.15.

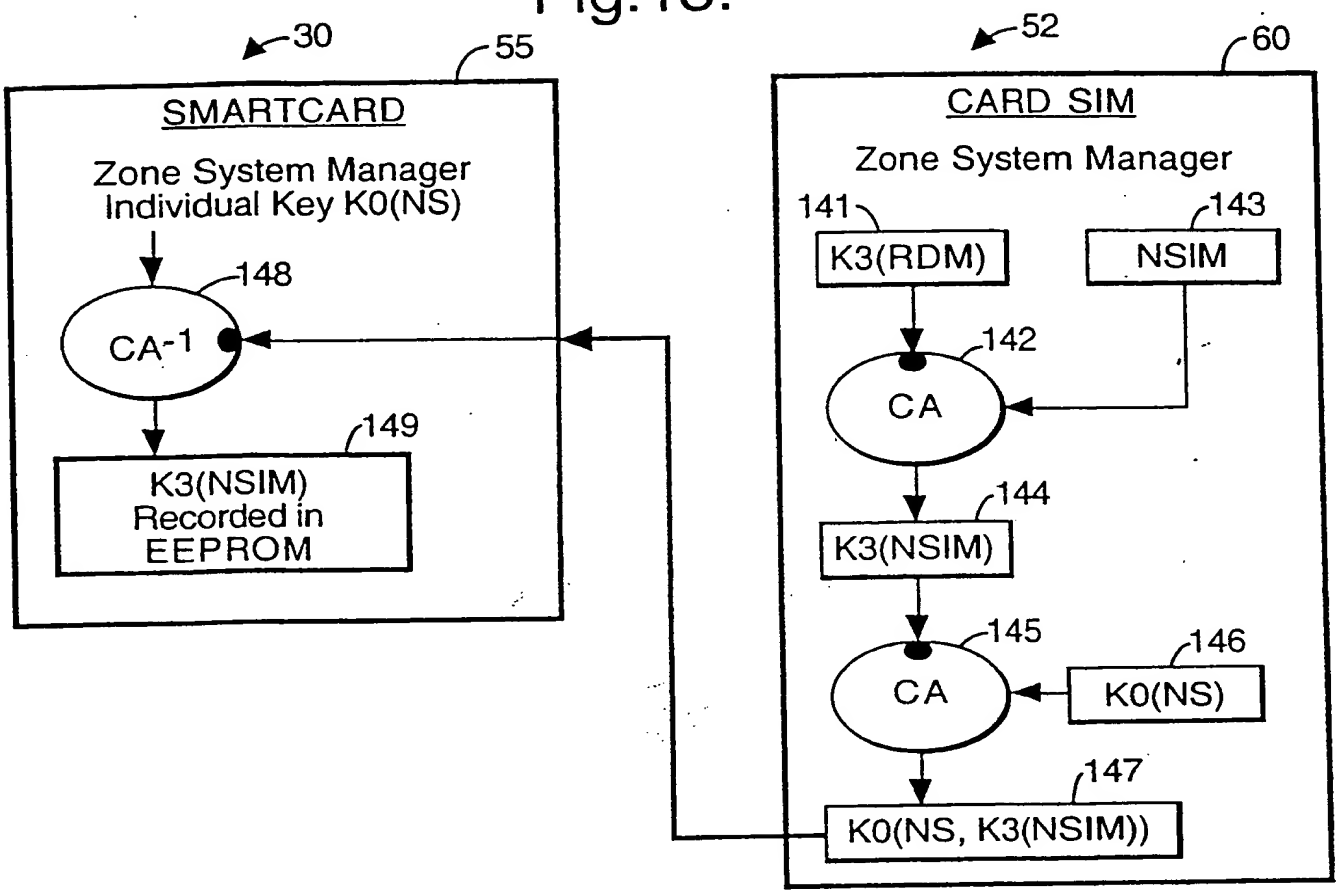

30
55
SMARTCARD
Zone System Manager
Individual Key K0(NS)
148
CA-1
149
K3(NSIM)
Recorded in
EEPROM
52
60
CARD SIM
Zone System Manager
141
K3(RDM)
143
NSIM
142
CA
144
K3(NSIM)
145
CA
146
K0(NS)
147
K0(NS, K3(NSIM))

Fig.16.

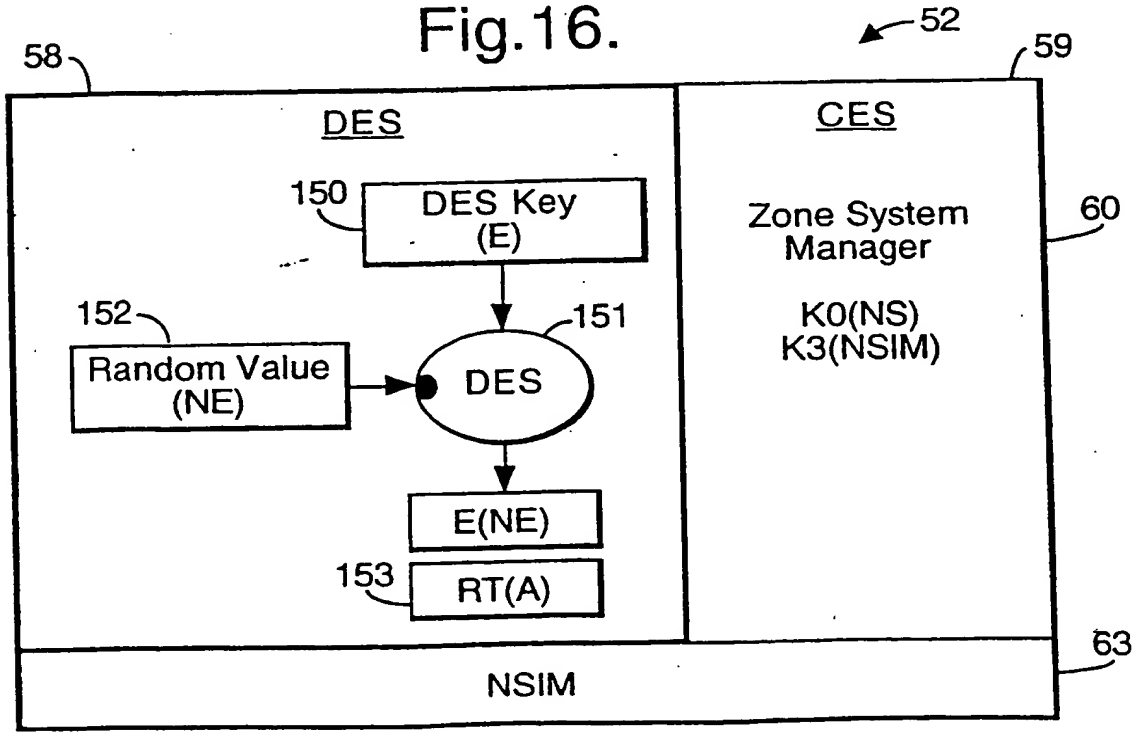

58
52
59
DES
CES
150
DES Key
(E)
Zone System
Manager
60
K0(NS)
K3(NSIM)
152
Random Value
(NE)
151
DES
E(NE)
153
RT(A)
63
NSIM

Fig.17.

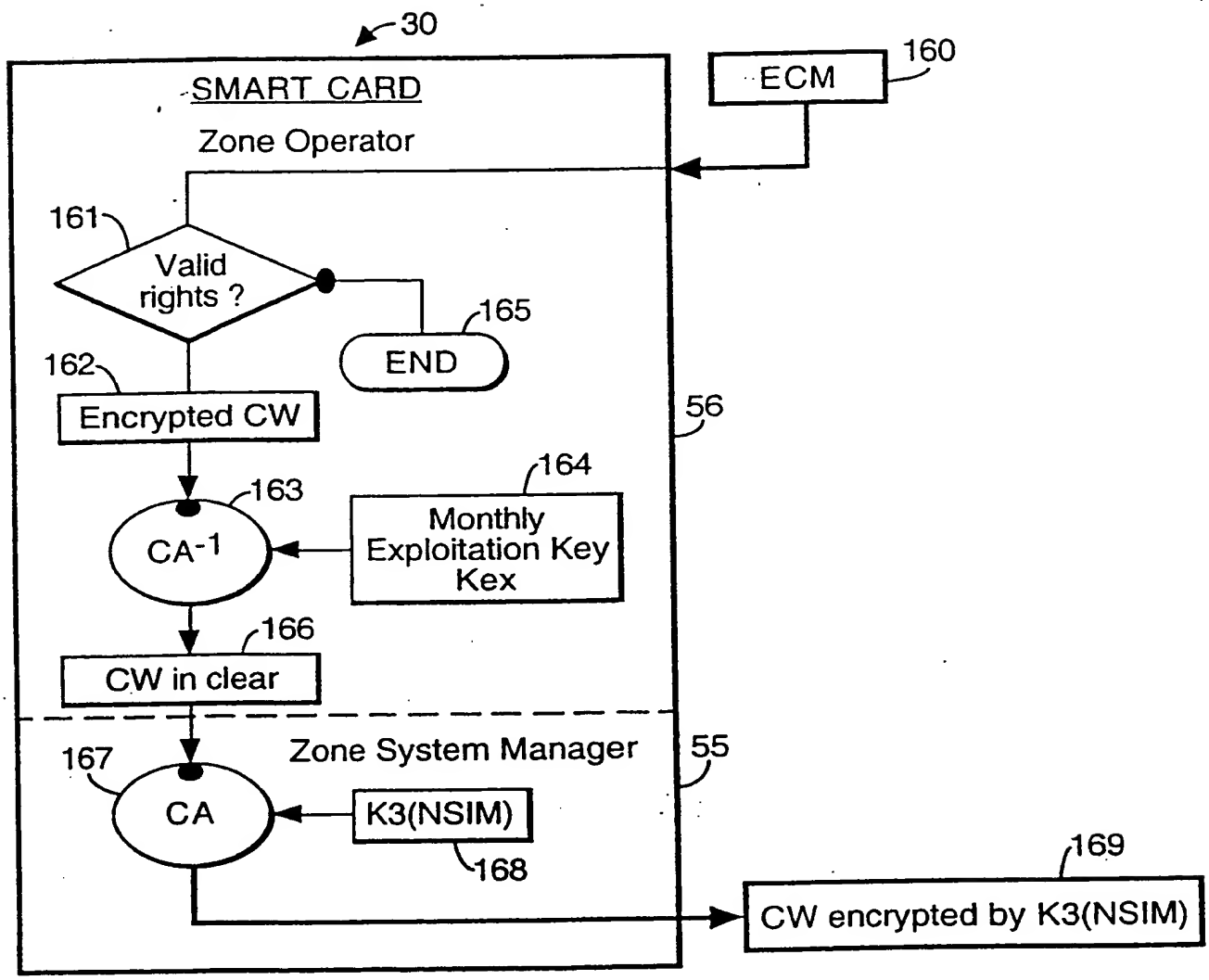

30
SMART CARD
Zone Operator
ECM
160
161
Valid rights ?
165
END
162
Encrypted CW
56
164
163
CA-1
Monthly Exploitation Key Kex
166
CW in clear
Zone System Manager
55
167
CA
K3(NSIM)
168
169
CW encrypted by K3(NSIM)

Fig.18.

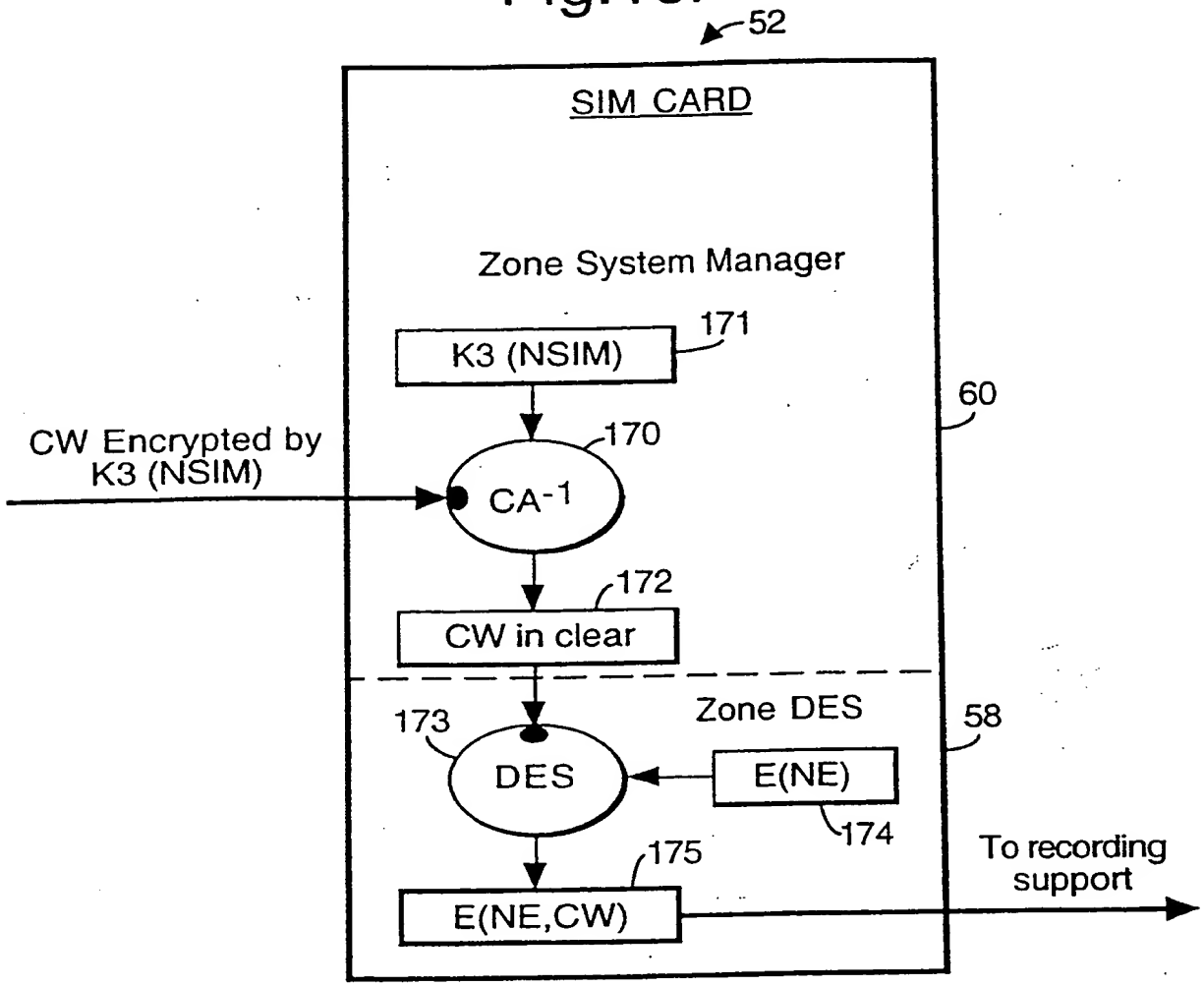
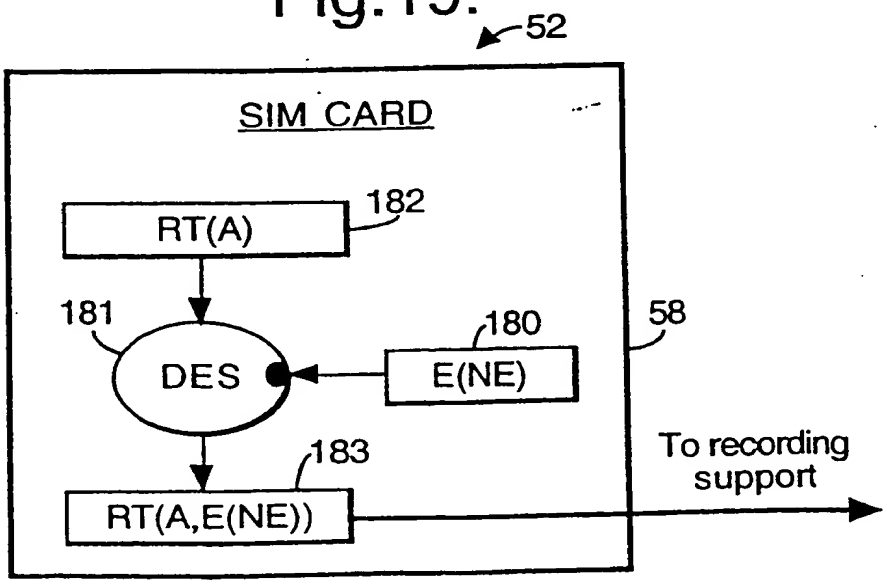

52
SIM CARD
Zone System Manager
K3 (NSIM)
171
60
CW Encrypted by K3 (NSIM)
170
CA-1
172
CW in clear
Zone DES
173
58
DES
E(NE)
174
175
To recording support
E(NE,CW)

Fig.19.


52
SIM CARD
RT(A)
182
181
180
58
DES
E(NE)
183
To recording support
RT(A,E(NE))

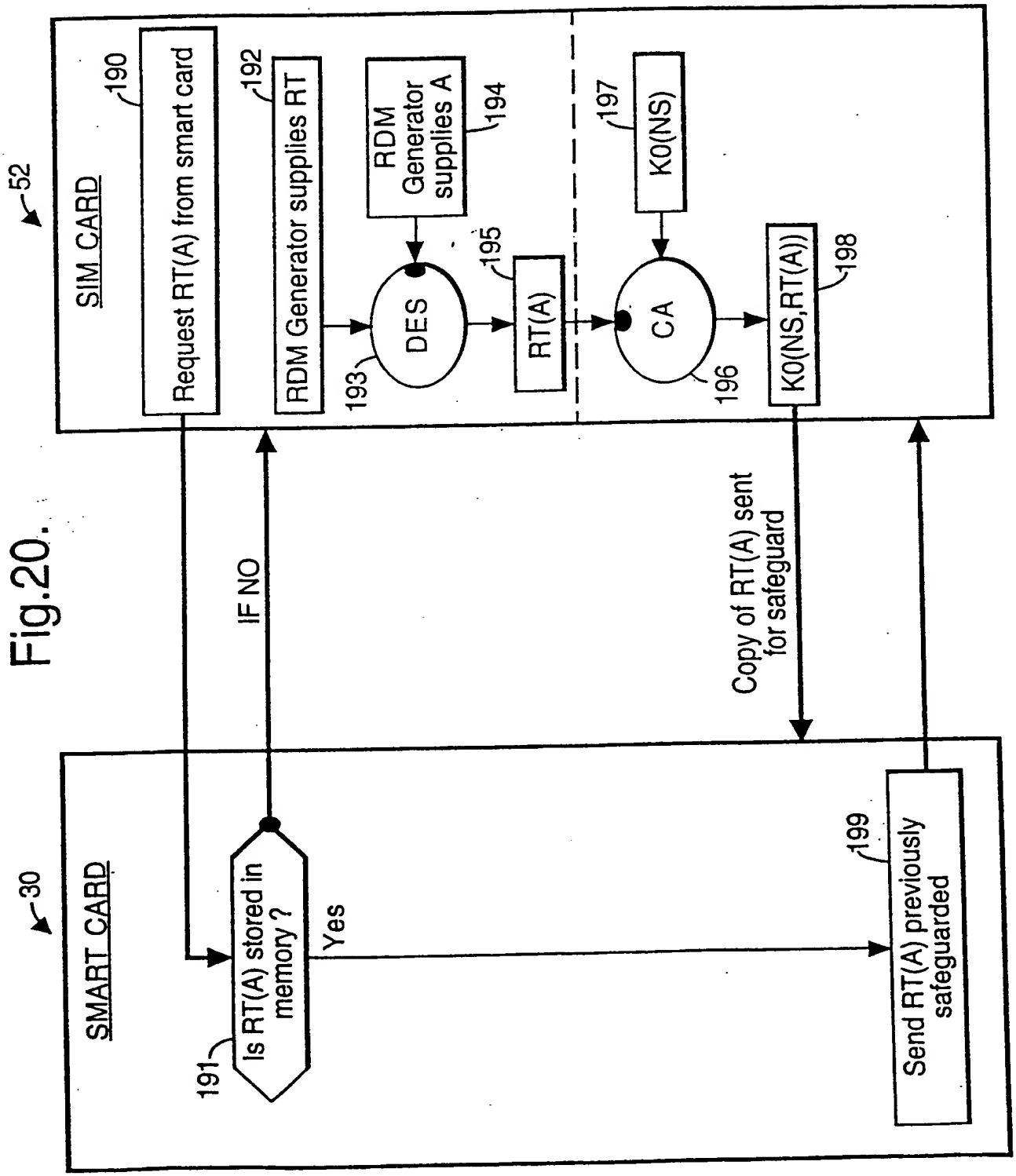

52
SIM CARD
190
Request RT(A) from smart card
192
RDM Generator supplies RT
RDM Generator supplies A
194
197
K0(NS)
193
DES
195
RT(A)
CA
196
K0(NS,RT(A))
198
IF NO
Copy of RT(A) sent for safeguard
30
SMART CARD
191
Is RT(A) stored in memory ?
Yes
199
Send RT(A) previously safeguarded

Fig.20.